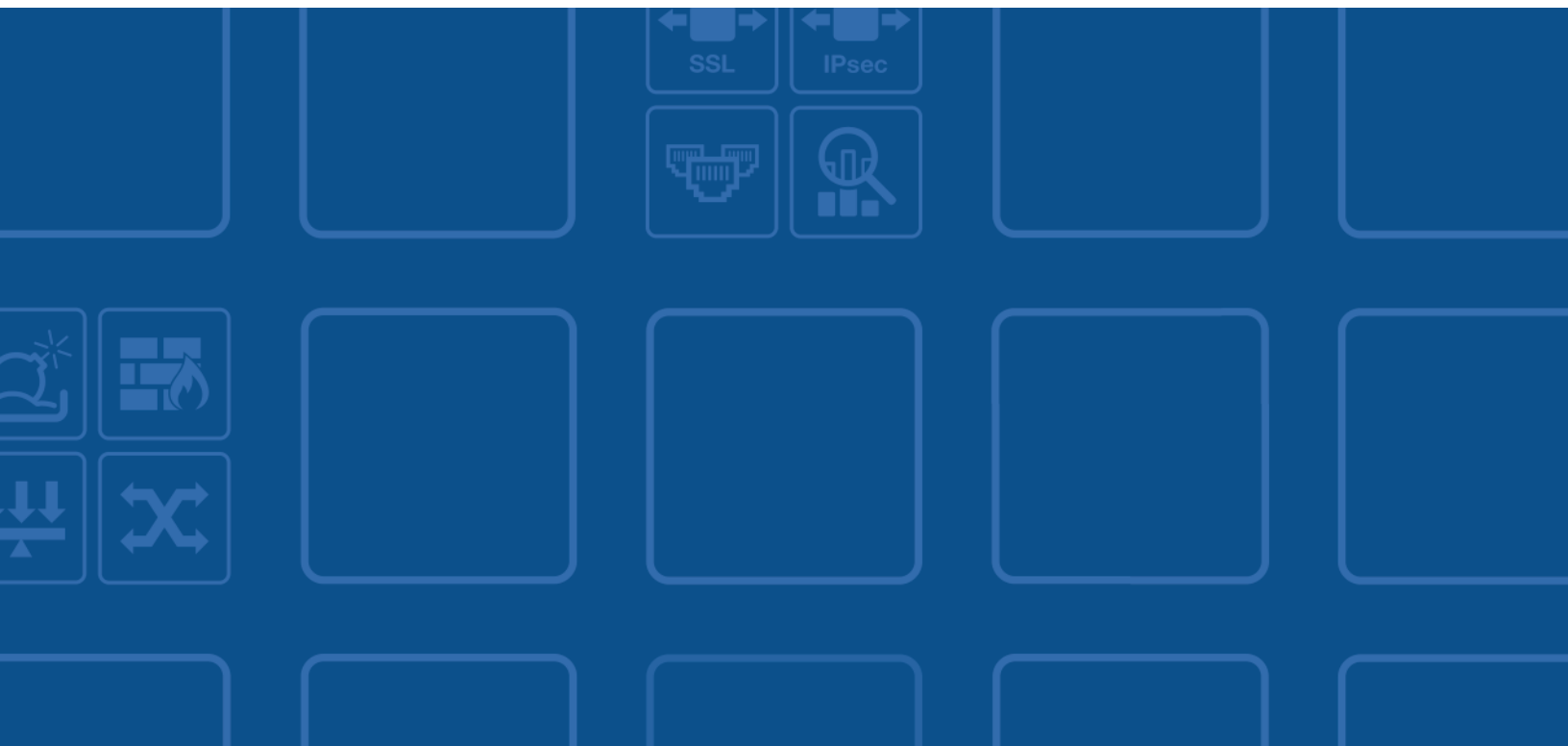
FortiManager - Upgrade Guide

VERSION 5.4.4



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 25, 2017

FortiManager 5.4.4 Upgrade Guide

02-544-446902-20170725

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-10-05	Initial Release.
2017-10-16	Added *Upgrading ADOMs* topic.
2017-07-25	Added FMG-300F to *FortiManager Firmware Upgrade Paths and Supported Models* topic.

Introduction

This document describes how to upgrade FortiManager to 5.4.4. This guide is intended to supplement the *FortiManager Release Notes*, and it includes the following sections:

Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiManager Release Notes*, or contact Fortinet Customer Service & Support (https://support.fortinet.com/).

Preparing to Upgrade FortiManager

This section describes how to prepare FortiManager for upgrade. It includes a summary and details of each preparation task.

Summary of preparation tasks

We recommend performing the following tasks to prepare for a successful upgrade of a FortiManager unit. This section provides a summary of the tasks and includes links to the details for each task.

To prepare for upgrading FortiManager (summary):

1. Download release notes, firmware images, and SNMP MIB files. See Downloading files from Customer Service & Support on page 7.
2. Review release notes. See Reviewing FortiManager 5.4.4 Release Notes on page 10.
3. Plan when to perform the upgrade. See Planning when to upgrade on page 10.
4. Install pending configuration files. See Installing pending configurations on page 10.
5. Review the status of managed devices. See Reviewing status of managed devices on page 10.
6. Check the status of FortiManager databases. See Checking FortiManager databases on page 12.
7. Review FortiManager System Settings pane. See Reviewing FortiManager System Settings on page 15.
8. Back up configuration files and databases. See Backing up configuration files and databases on page 16.
9. Clone VM instances. See Creating a snapshot of VM instances on page 17.

Upgrading ADOMs

If you have ADOMs that are earlier than version 5.0, upgrade these ADOMs to a supported version. Supported ADOM versions are 5.0, 5.2, and 5.4.

To upgrade ADOM version:

1. In the older version ADOM, upgrade one of the FortiGate units to FortiOS 5.0 or later, and then resynchronize the device.
   All the ADOM objects, including Policy Packages, remain as 5.0 objects.
2. Upgrade the rest of the FortiGate units in the older version ADOMs to FortiOS 5.0 or later.
3. Upgrade the ADOM to version 5.0 or later.
   a. Ensure that you are logged into FortiManager as a super user administrator.
   b. Go to *System Settings* > *All ADOMs*.
   c. Right-click an ADOM and select *Upgrade*.
   d. Click *OK* in the confirmation dialog box to upgrade the device.

If all the devices in the ADOM are not already upgraded, the upgrade is aborted and an error message is displayed. Upgrade the remaining devices in the ADOM and then upgrade the ADOM again.

All the database objects are converted to the new version's format and the GUI content for the ADOM changes to reflect the new version's features and behavior.

For more information, see the *FortiManager Administration Guide*.

Downloading files from Customer Service & Support

You can download release notes and firmware images from the Fortinet Customer Service & Support portal at https://support.fortinet.com. If you are using SNMP to monitor equipment, you can also download MIB files from the Fortinet Customer Service & Support portal.

This section also describes the VM firmware images available for FortiManager.

Downloading release notes and firmware images

Firmware images are located on the Fortinet Customer Service & Support portal, and they are organized by firmware version, major release, and patch release.

For information about the naming convention of firmware images and VM firmware images, see FortiManager firmware images on page 8, FortiManager VM firmware images on page 9, and Build numbers on page 10.

We recommend running an MD5 checksum on the firmware image file.

To download release notes and firmware images:

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select *FortiManager*.
4. Download the release notes for the 5.4.4 build:
   a. On the *Release Notes* tab, click the *5.4.4 Build <number>* link.
      The Document Library is displayed.
   b. Download the release notes.
5. Download the firmware image:
   a. Return to the Fortinet Customer Service & Support portal, and click the *Download* tab.
   b. Go to the *v5.00* > *5.4* > *5.4.4* folder, and locate the firmware image for your device or VM.
   c. Download the firmware image by clicking the *HTTPS* link.
      An HTTPS connection is used to download the firmware image.
   d. Click the *Checksum* link for the image that you downloaded.
      The image file name and checksum code are displayed in the *Get Checksum Code* dialog box.
   e. Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.

Downloading MIB files

If you are not using SNMP to monitor equipment, you can skip this procedure.

If you are using SNMP to monitor equipment, download the following MIB files from the Fortinet Customer Service & Support portal:

- *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib*, which is used with both FortiManager and FortiAnalyzer
- Fortinet Core MIB file, which is used with all Fortinet products

To download SNMP MIB files:

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select *FortiManager*.
4. Download the MIB file for the FortiManager 5.4.4 release:
   a. On the *Download* tab, go to the *v5.00* > *5.4* > *5.4.4* > *MIB* folder.
   b. Download the MIB file by clicking the *HTTPS* link.
      An HTTPS connection is used to download the firmware image.
   c. Click the *Checksum* link for the image that you downloaded.
      The image file name and checksum code are displayed in the *Get Checksum Code* dialog box.
   d. Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.
5. Download the Fortinet Core MIB file:
   a. On the *Download* tab, go to the *v5.00* > *Core MIB* folder.
   b. Download the MIB file by clicking the *HTTPS* link.
      An HTTPS connection is used to download the firmware image.
   c. Click the *Checksum* link for the image that you downloaded.
      The image file name and checksum code are displayed in the *Get Checksum Code* dialog box.
   d. Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.

FortiManager firmware images

The firmware images in the folders follow a specific naming convention, and each firmware image is specific to the device model or VM.

For example, the FMG_1000C-v5-build1187-FORTINET.out image found in the */FortiManager/v5.00/5.4/5.4.3/* file folder is specific to the FortiManager 1000C device model.

FortiManager VM firmware images

Fortinet provides FortiManager VM firmware images for Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available in the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: For a new FortiManager VM installation, also download the Hyper-V package as it contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.ovf.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information, see the FortiManager data sheet at https://www.fortinet.com/products/management/fortimanager.html.

VM installation guides are available in the Fortinet Document Library.

Build numbers

Firmware images are generally documented as build numbers. New models may be released from a branch of the regular firmware release. As such, the build number found in the *System Settings > General > Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch Point` field that displays the regular build number.

Ensure that FortiManager 5.4.4 can run on your FortiManager model. See FortiManager Firmware Upgrade Paths and Supported Models on page 23.

Reviewing FortiManager 5.4.4 Release Notes

After you download the release notes for FortiManager 5.4.4, review the special notices, upgrade information, product integration and support, resolved issues, and known issues.

Planning when to upgrade

Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or managed devices.

Installing pending configurations

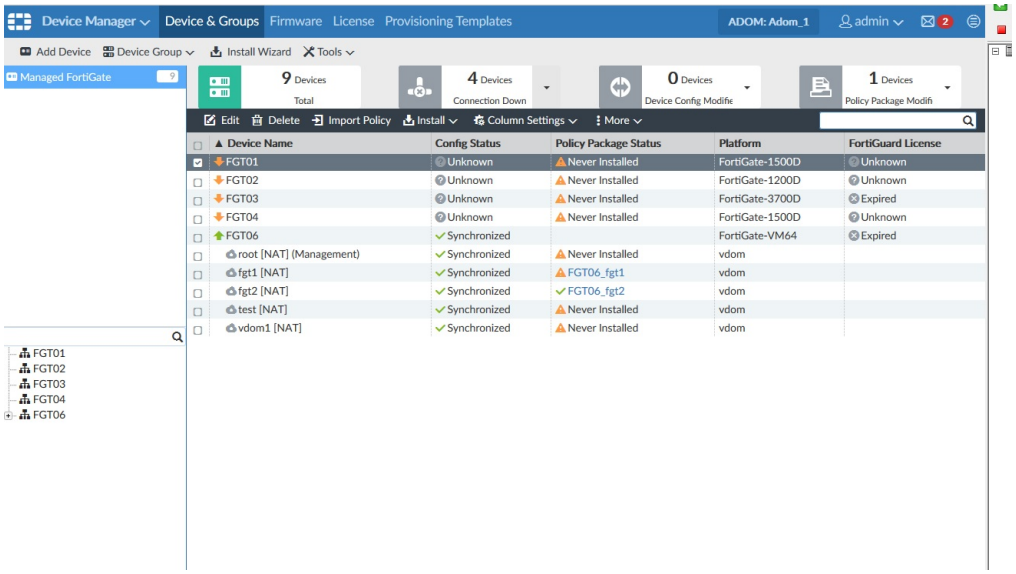
Prepare your device for upgrade by installing any pending configurations, and ensure that your managed devices are running the appropriate firmware versions as documented in the firmware Release Notes.

Reviewing status of managed devices

Before starting an upgrade, use the *Device Manager* pane to review the status of all managed devices to ensure they have a status of *In Sync*.

Either correct devices without an *In Sync* status or make note of them prior to starting the upgrade.

Following is an example of the *Device Manager* pane:



Also, you can use the following CLI commands to gather detailed properties of managed devices, device groups, or ADOMs. The example output that follows highlights the important properties and attributes.

- `diagnose dvm adom list`
- `diagnose dvm device list`
- `diagnose dvm group list`

CLI example of diagnose dvm adom list

Following is an example of the CLI output for the `diagnose dvm adom list` command:

```
# diagnose dvm adom list
There are currently 26 ADOMs:
OID STATE PRODUCT OSVER MR NAME MODE VPN MANAGEMENT IPS
...
...
239 enabled FOS 5.0 4 54-ADOM Normal Policy & Device VPNs 10.00032 (regular)
141 enabled FOS 5.0 4 54-VPN Normal Central VPN Console 6.00741 (regular)
...
...
---End ADOM list---
```

The following properties should be the same before and after the upgrade:

- Total number of ADOMs.
- Name of each ADOM.
- VPN management mode. There are two VPN management modes: `Policy & Device VPNs` or `Central VPN Console`.

CLI example of diagnose dvm device list

Following is an example of the CLI output for the `diagnose dvm device list` command:

```
# diagnose dvm device list
--- There are currently 16 devices/vdoms managed ---
TYPE            OID SN               HA IP         NAME    ADOM    IPS
...
...
fmg/faz enabled 448 FGVM020000058807 - 10.3.121.82 FGVM82 54-VPN 6.00741 (regular)
|- STATUS: db: modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:54-VPN pkg:[modified]pp_vpn_v1
fmg/faz enabled 317 FGVM02Q105060033 - 10.3.121.92 FGVM92 54-ADOM 6.00741 (regular)
|- STATUS: db: not modified; conf: out of sync; cond: unknown; dm: autoupdated; conn: down
|- vdom:[3]root flags:1 adom:54-ADOM pkg:[unknown]VM92_root
...
...
--- End device list ---
```

This command shows the total number of devices or VDOMs, the configuration status of devices and policy packages, and the connection status. The number of managed devices or VDOMs should be the same before and after the upgrade.

- If the device configuration or policy package status (`db`) is `modified`, we recommend installing the changes before upgrading.
- The policy package status (`pkg`) shows if there is any pending package change on a policy package that has been linked to a device or VDOM. This status can be `modified`, `never-installed`, or `unknown`.
- The connection status (`conn`) is either `up` or `down`.

CLI example of diagnose dvm group list

Following is an example of the CLI output for the `diagnose dvm group list` command:

```
FMG-v54 # diagnose dvm group list
There are 2 groups:
OID  NAME          ADOM
277  FGT_Group1    54-VPN
+DEVICE oid=162 name=FGTVM93
278  FGT_Group2    54-VPN
+DEVICE oid=265 name=FGTVM94
---End group list---
```

The number of groups and their members should be the same before and after the upgrade.

Checking FortiManager databases

Before upgrading, we recommend checking the integrity of FortiManager databases using the following CLI commands. If you find any errors, you can fix the errors before starting the upgrade. If you need to fix database errors, back up before making any changes. See Backing up configuration files and databases on page 16.

If workspace mode is enabled, you must unlock all ADOMs before running any integrity commands. For information on workspace mode, see the *FortiManager Administration Guide*.

diagnose pm2 check-integrity all

Check the integrity of the Policy Manager database by using the following command: `diagnose pm2 check-integrity all`.

The `diagnose pm2 check-integrity all` command only detects errors. It cannot correct errors. If any errors are found, the only option is to restore from the last good backup before upgrading.

Example 1 with error:

```
FMG-VM64 # diagnose pm2 check-integrity all
--- pragma integrity_check adom db ---
Error: database disk image is malformed
pragma integrity_check fails: /var/pm2/adom153
>>> total: 10 failed: 1
```

Example 2 without error:

```
FMG-VM64 # diagnose pm2 check-integrity all
--- pragma integrity_check adom db ---
--- total: 15 ok.
--- pragma integrity_check device db ---
--- total: 1 ok.
--- pragma integrity_check global db ---
--- total: 2 ok.
--- pragma integrity_check ips db ---
--- total: 3 ok.
--- pragma integrity_check task db ---
--- total: 1 ok.
--- pragma integrity_check ncmdb db ---
--- total: 18 ok.
```

diagnose dvm check-integrity

Check the integrity of the Device Manager database by using the following command: `diagnose dvm check-integrity`.

Example 1 with error:

```
FMG-VM64 # diagnose dvm check-integrity
[1/8] Checking object memberships ... correct
[2/8] Checking device nodes ... 0 change(s) will be made (263 error(s))
[3/8] Checking device vdoms ...
...
The above changes will be made to the database, however it is recommended to perform a
    backup first.
Do you want to continue? (y/n)
```

Example 2 without error:

```
FMG-VM64 # diagnose dvm check-integrity
[1/8] Checking object memberships       ... correct
[2/8] Checking device nodes             ... correct
```

```
[3/8] Checking device vdoms             ... correct
[4/8] Checking duplicate device vdoms   ... correct
[5/8] Checking device ADOM memberships  ... correct
[6/8] Checking groups                   ... correct
[7/8] Checking group membership         ... correct
[8/8] Checking task database            ... correct
```

diagnose cdb check adom-integrity

Check the integrity of the object configuration database by using the following command: `diagnose cdb check adom-integrity`.

This command does not work on version 5.4.3 or versions earlier than 5.2.11.

Example 1 with error:

```
FMG-VM64 # diagnose cdb check adom-integrity
General updating - adom FWF_LAB    ... ..100% Ready to update
General updating - adom FWF_Root   ... ..100% Ready to update
General updating - adom root       ... ..100% An error has occured: (errno=33):duplicate
If the update check returns an error, please contact Fortinet Support for assistance.
```

Example 2 without error:

```
FMG-VM64 # diagnose cdb check adom-integrity
General updating - adom FWF_Root     ... .......90%..100% Ready to update
General updating - adom FWF_ADOM_50  ... .......90%..100% Ready to update
General updating - adom FWF_ADOM_52  ... ...........90%..100% % Ready to update
General updating - adom root         ... ...100% Ready to update
```

diagnose cdb check policy-assignment

Check the integrity of the global policy assignment table by using the following command: `diagnose cdb check policy-assignment`.

Example:

```
FMG-VM64 # diagnose cdb check policy-assignment
Checking global policy assignment ... correct
```

diagnose cdb check objcfg-integrity

Check the integrity of the object configuration database table by using the following command: `diagnose cdb check objcfg-integrity`.

Example:

```
FMG-VM64 # diagnose cdb check objcfg-integrity
Checking object config database table columns ... correct
```

diagnose cdb check reference-integrity

Check the integrity of the ADOM reference table by using the following command: `diagnose cdb check reference-integrity`.

Example:

```
FMG-VM64 # diagnose cdb check reference-integrity
Checking reference table integrity ... correct
```

diagnose cdb check policy-packages

Check the integrity of the ADOM reference table by using the following command: `diagnose cdb check policy-packages`.

Example 1 with error:

```
FMG-VM64 # diagnose cdb check policy-packages
Adom VPNConsole
   [1/3] Checking Scope ... correct
   [2/3] Checking Dynamic mappings ... 2 change(s) will be made
   [3/3] Checking Policy package settings ... correct
Adom root
   [1/3] Checking Scope ... correct
   [2/3] Checking Dynamic mappings ... correct
   [3/3] Checking Policy package settings ... correct
The above change(s) will be made to the database, however it is recommended to perform a
    backup first.
Do you want to continue? (y/n)
```

Example 2 without error:

```
FMG-VM64 # diagnose cdb check policy-packages
Adom FG54
   [1/3] Checking Scope ... correct
   [2/3] Checking Dynamic mappings ... correct
   [3/3] Checking Policy package settings ... correct
Adom root
   [1/3] Checking Scope ... correct
   [2/3] Checking Dynamic mappings ... correct
   [3/3] Checking Policy package settings ... correct
```

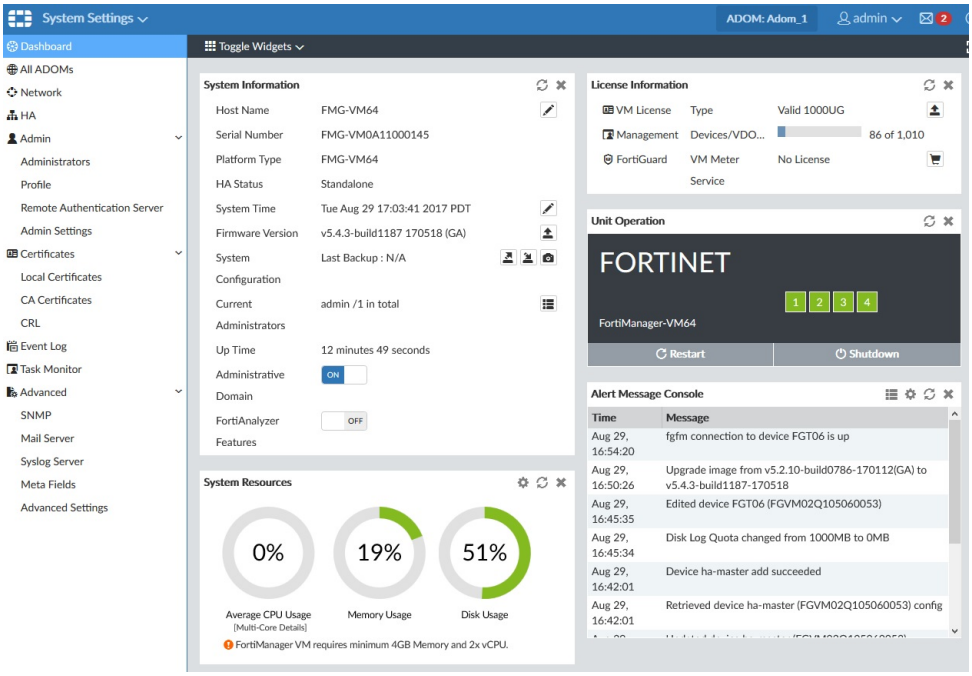
Reviewing FortiManager System Settings

Before starting an upgrade, go to *System Settings* to review the following widgets:

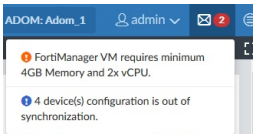
- License Information widget
- System Resources widget to check for high memory and CPU usage

It is also recommended to check the Alert Message Console and the list of notifications.

Following is an example of the *System Settings Dashboard* with the *License Information* and *System Resources* widgets:



Following is an example of the Notification list:



Backing up configuration files and databases

Back up the FortiManager configuration file and databases.

It is recommended that you create a system backup file and save this configuration to your local computer. The device configuration file is saved with a `.dat` extension.

It is also recommended that you verify the integrity of your backup file.

When the database is larger than 2.8 GB, back up the configuration file to an FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename
    of server> <username on server> <password> <crptpasswd>

execute backup all-settings scp <ip> <path/filename of
    server> <SSH certificate> <crptpasswd>
```

For more information, see the *FortiManager CLI Reference*.

To verify the integrity of a backup file:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click *Backup*. The *Backup* dialog box opens.
3. In the `Encryption` line, deselect the checkbox so that the backup is not encrypted.
4. Click *OK* and save the backup file on your local computer.
5. Locate the backup file and change the file extension from `.dat` to `.tgz`.
6. Decompress the backup file and verify that the decompression is successful.

If the decompression fails, then the backup process has likely also failed.

Ensure the backup is not encrypted because an encrypted backup always fails to decompress.

To back up your system configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click *Backup*. The *Backup* dialog box opens.
3. If you wish, select the checkbox to encrypt the backup file, and enter a password.
4. Click *OK* and save the backup file on your local computer.

If you encrypt the backup file, you must use the same password to restore this backup file.

Creating a snapshot of VM instances

In VM environments, it is recommended to take a snapshot or clone of the VM instance before the upgrade. In the event of an issue with the upgrade, you can revert to the VM snapshot or clone.

Upgrading FortiManager

You can upgrade FortiManager 5.2.0 or later directly to FortiManager 5.4.4.

If you are upgrading from versions earlier than 5.2.0, you must upgrade to FortiManager 5.2 first. We recommend that you upgrade to the latest version of FortiManager 5.2.

See also FortiManager Firmware Upgrade Paths and Supported Models on page 23.

During firmware upgrade, all ADOMs (and Policy Package Versions, if ADOMs are disabled) remain at the same version as before the upgrade. For information about upgrading ADOMs, see the *FortiManager Administration Guide*.

Upgrading the device firmware can trigger an SQL database rebuild. New logs are not be available until the rebuild is complete. The time required to rebuild the database depends on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features are available until the SQL database rebuild is complete: FortiView, Log View, Event Management, and Reports.

Upgrading FortiManager Firmware

This section describes how to upgrade FortiManager firmware.

It is recommended to upload firmware to FortiManager by using a server that is in the same location as the FortiManager. This helps avoid timeouts.

When upgrading from FortiManager 5.4.0 to 5.4.4, reboot FortiManager 5.4.0 before installing the firmware image for FortiManager 5.4.4.

To upgrade firmware:

1. Enable offline mode in *System Settings* > *Advanced* > *Advanced Settings*.
   Offline mode stops automatic firmware updates during the upgrade.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, go to the *Firmware Version* field, and click the *Upgrade Firmware* icon.
   The *Firmware Upload* dialog box displays.
4. Click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal, and click *Open*.
5. Click *OK*.

The firmware image is uploaded. When the upgrade completes, a confirmation message is displayed that communicates a successful upgrade.

It is recommended to view the console log output during upgrade. See Checking FortiManager log output on page 19.

6. Once the login window is displayed, log into FortiManager.
7. Disable offline mode in *System Settings* > *Advanced* > *Advanced Settings*.
8. Review the *System Settings* > *Event Log* for any additional errors. See Checking FortiManager events on page 20.

Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server>
    <IP of server> <username on server> <password>
```

For more information, see the *FortiManager CLI Reference*.

Upgrading the firmware for an operating cluster

You can upgrade the firmware of an operating cluster through the GUI or CLI of the primary unit.

Similar to upgrading the firmware of a standalone unit, normal operations are temporarily interrupted during the cluster firmware upgrade. Therefore, you should upgrade the firmware during a maintenance window.

To upgrade an HA cluster:

1. Log into the GUI of the primary unit using the `admin` administrator account.
2. Upgrade the primary unit firmware. The upgrade is automatically synchronized between the primary device and backup devices.

   It is recommended to view the console log output during upgrade. See Checking FortiManager log output on page 19.

Administrators may be unable to connect to the GUI until the upgrade synchronization process is completed. During the upgrade, SSH or telnet connections to the CLI may also be slow. You can still use the console to connect to the CLI of the primary device.

Checking FortiManager log output

While upgrading a FortiManager unit, use the console to check the log output in real-time. Check for any errors or warnings.

Following is a sample console output with warnings or errors you might encounter during an upgrade:

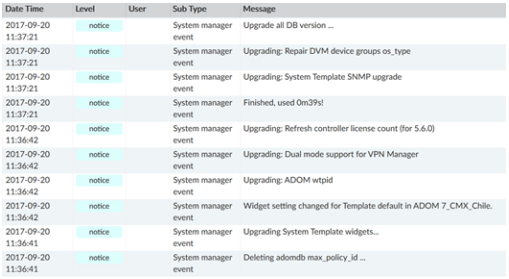
```
Please stand by while rebooting the system.
Restarting system.
Serial number:FMG-VM0A11000137
Upgrading sample reports...Done.
```

```
Upgrading geography IP data...Done.
rebuilding log database (log storage upgrade)...
Prepare log data for SQL database rebuild...Done.
Global DB running version is 222, built-in DB schema version is 432
......
upgrading device ssl-vpn flags...done
upgrading scripts ...
Invalid schedule. The device 10160520 does not belong to script 136's adom
Invalid schedule. The device 33933609 does not belong to script 46's adom
Invalid schedule. The device 10515974 does not belong to script 46's adom
......
Invalid schedule. The device 1709397 does not belong to script 46's adom
Invalid schedule. The device 1709397 does not belong to script 46's adom
Invalid schedule. The device 1407292 does not belong to script 46's adom
upgrading scripts ... done
upgrading script log ...
Failed to upgrade some script logs. Please use "diagnose debug backup-oldformat-script-
    logs" to upload the failed logs into a ftp server
upgrading script log ... done
Upgrading adom vpn certificate ca ...
......
Finish check-upgrade-objects [32923/49325]
Upgrade all DB version ...
Global DB running version is upgraded to 432
Database upgrade finished, using 846m11s
```

Checking FortiManager events

After upgrading, it is recommended to check all messages logged to the FortiManager Event Log. If you find any errors, you can fix the errors before continuing.

Following is an example of messages in the FortiManager Event Log:



Date Time	Level	User	Sub Type	Message
2017-09-20 11:37:21	notice		System manager event	Upgrade all DB version ...
2017-09-20 11:37:21	notice		System manager event	Upgrading: Repair DVM device groups os_type
2017-09-20 11:37:21	notice		System manager event	Upgrading: System Template SNMP upgrade
2017-09-20 11:37:21	notice		System manager event	Finished, used 0m39s!
2017-09-20 11:36:42	notice		System manager event	Upgrading: Refresh controller license count (for 5.6.0)
2017-09-20 11:36:42	notice		System manager event	Upgrading: Dual mode support for VPN Manager
2017-09-20 11:36:42	notice		System manager event	Upgrading: ADOM wtpid
2017-09-20 11:36:42	notice		System manager event	Widget setting changed for Template default in ADOM 7_CMX_Chile.
2017-09-20 11:36:41	notice		System manager event	Upgrading System Template widgets...
2017-09-20 11:36:41	notice		System manager event	Deleting adomdb max_policy_id ...

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

Verifying FortiManager Upgrade Success

Once the upgrade is complete, check the FortiManager unit to ensure that the upgrade was successful. This section describes items you should check.

Checking Alert Message Console and notifications

After the FortiManager upgrade completes, check the *Alert Message Console* and list of notifications for any messages that might indicate problems with the upgrade.

- In *System Settings* > *Dashboard*, check the *Alert Message Console* widget.
- Click the Notification icon and review any notifications.

For information on accessing system settings, see Reviewing FortiManager System Settings on page 15.

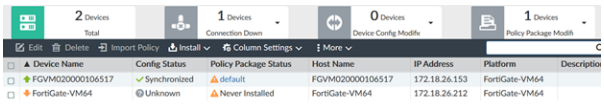
Checking managed devices

After the FortiManager upgrade completes, check the managed devices in the GUI.

To check managed devices:

1. Refresh the browser and log back into the device GUI.
2. Go to *Device Manager*, and ensure that all formerly added devices are still listed.
3. In *Device Manager*, select each ADOM and ensure that managed devices reflect the appropriate connectivity state.

   Following is an example of the quick status bar in *Device Manager* where you can check the connectivity status of managed devices. It might take some time for FortiManager to establish connectivity after the upgrade.



4. Launch other functional modules and make sure they work properly.

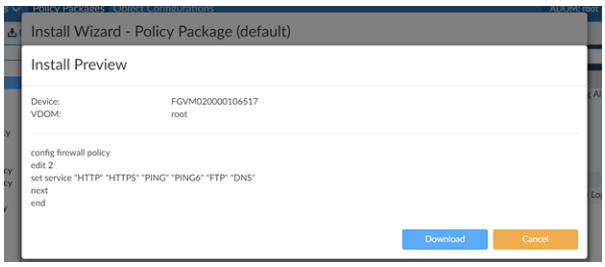
   See Previewing changes for a policy package installation on page 22.

Previewing changes for a policy package installation

The first time that you install a policy package after the upgrade, use the Install Preview feature to ensure that only the desired changes will be installed to the device.

The policy package must include a change to use the Install Preview feature.

Following is an example of the Install Preview pane:



FortiManager Firmware Upgrade Paths and Supported Models

For information about FortiManager support for FortiOS, see the FortiManager Compatibility chart in the Document Library at http://docs.fortinet.com/d/fortimanager-compatibility.

Before upgrading your device, see details in the applicable releases notes.

Firmware Version	Build Number	Upgrade From
5.4.4	1225	5.4.0–5.4.3 5.2.0–5.2.10
Note: With the enhancement in password encryption, FortiManager 5.4.4 does not support FortiOS 5.4.0. You need to upgrade FortiGate to 5.4.3 or later. ADOM versions 5.0 and 5.2 are not affected.		
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-300F, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV (including Hyper-V 2016), FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).		
5.4.3	1187	5.4.0–5.4.2 5.2.0–5.2.10
Note: With the enhancement in password encryption, FortiManager 5.4.3 does not support FortiOS 5.4.0. You need to upgrade FortiGate to 5.4.2 or later. ADOM versions 5.0 and 5.2 are not affected.		
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).		
5.4.2	1151	5.4.0–5.4.1 5.2.0–5.2.9
Note: With the enhancement in password encryption, FortiManager 5.4.2 does not support FortiOS 5.4.0. You need to upgrade FortiGate to 5.4.2. ADOM versions 5.0 and 5.2 are not affected.		
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).		

Firmware Version	Build Number	Upgrade From
5.4.1	1082	5.4.0 5.2.0–5.2.7
Note: With the enhancement in password encryption, FortiManager 5.4.1 does not support FortiOS 5.4.0. You need to upgrade FortiGate to 5.4.1. ADOM versions 5.0 and 5.2 are not affected.		
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).		
5.4.0	1019	5.2.0–5.2.4
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).		
5.2.9	0780	5.2.0–5.2.7 5.0.6–5.0.10
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM64, FMG64-AWS, FMG-VM64-HV, FMGVM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).		
5.2.7	0757	5.2.0–5.2.6 5.0.6–5.0.10
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMG-VM64-KVM, FMG64-AWS, and FMG-VM64-HV.		
5.2.6	0753	5.2.0–5.2.4 5.0.6–5.0.10
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG64-AWS, and FMG-VM64-HV.		

Firmware Version	Build Number	Upgrade From
5.2.4	0738	5.2.0–5.2.3 5.0.6–5.0.10
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG-VM64-AWS, and FMG-VM64-HV.		
5.2.3	0724	5.2.0–5.2.2 5.0.6–5.0.10
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM, FMG-VM64-AWS, and FMG-VM64-HV.		
5.2.2	0706	5.2.0–5.2.2 5.0.6–5.0.10
Supported models: FMG-100C, FMG-200D, FMG-200E, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG-VM64-AWS, and FMG-VM64-HV.		
5.2.1	0662	5.2.0 5.0.8, 5.0.9
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, and FMG-VM64-HV.		
5.2.0	0618	5.0.6–5.0.9
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, and FMG-VM64-HV.		
5.0.12	0383	5.0.6–5.0.11
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-3900E, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMGVM64-KVM, and FMG-VM64-XEN.		
5.0.11	0377	5.0.6–5.0.10
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-3900E, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMGVM64-KVM, and FMG-VM64-XEN.		

Firmware Version	Build Number	Upgrade From
5.0.10	0365	5.0.6–5.0.9
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMGVM64-KVM, and FMG-VM64-XEN.		
5.0.9	0345	5.0.6–5.0.8
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.		
5.0.8	0329	5.0.6, 5.0.7
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.		
5.0.7	0321	5.0.6
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.		
5.0.6	0310	5.0 or later 4.3.0 or later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV. FMG-4000E is released on build 4046.		
5.0.5	0266	5.0 or later 4.3.0 or later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.		

Firmware Version	Build Number	Upgrade From
5.0.4	0232	5.0 or later 4.3.0 or later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.		
5.0.3	0200	5.0 or later 4.3.0 or later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D,FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV. FMG-VM64-HV is released on build 0200. FMG-1000D is released on build 4035.		
5.0.2	0151	5.0 or 5.0.1 4.3.0 or later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-400D, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. FMG-300D is released on build 4020. FMG-4000D is released on build 4019.		
5.0.1	0121	5.0.0 4.3.0 or later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. FMG-300D is released on build 4009.		
5.0.0	0076	4.3.0 or later
Supported models: FMG-100C, FMG-200D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.		

In FortiManager 5.0 and later, FortiClient endpoint agent configuration and management are handled by FortiGate Endpoint Control. You can configure your FortiGate to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. This feature requires a FortiGate running FortiOS version 5.0 or later.

For more information, see the *Device and Client Reputation for FortiOS 5.0 Handbook* in the Fortinet Document Library.

FortiManager 5.0 and later uses a new hard disk drive partition layout. After upgrading from pre-version 5.0 to 5.0 or later, you must make a backup and then reformat the disk with this command:

```
execute format {disk | disk-ext4 | disk-ext3}
```

Formatting the disk erases all local logs and FortiGuard database information. Back up any local event logs you wish to keep. The device will have to re-download all the AV/IPS/AS/WF objects from the FortiGuard Distribution Servers (FDS). This download might take up to half a day. During that time, managed devices cannot obtain these services from FortiManager, so during this time, configure devices to point to a backup FortiManager or the FDS for these services.